Requested Patent: JP11234259A

Title:

OTHER PARTY AUTHENTICATION AND KEY DELIVERY METHOD, DEVICE USING THE METHOD, CRYPTOGRAPHY COMMUNICATION METHOD AND SYSTEM THEREFOR ;

Abstracted Patent: JP11234259 ;

Publication Date: 1999-08-27 ;

Inventor(s): AIKAWA SHIN;; TAKARAGI KAZUO ;

Applicant(s): HITACHI LTD ;

Application Number: JP19980031635 19980213 ;

Priority Number(s): ;

IPC Classification: H04L9/08; G09C1/00; G09C1/00; H04L9/32 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To improve the efficiency of other party authentication and key deliv ery by preparing a response by mutually using an irreversible compression function (a hash function) or a common key cryptography based on random numbers of the other party and by mutually exchanging its response.SOLUTION: Equipment A101 calculates a response rA based on rA=h (KBverbar verbar nAverbar verbar nB) by using random numbers kB, nA and nB. An arithmetic operation Xverbar verbar Y denotes that bit sequences X and Y are connected and a function h(X) denotes a hash function. Next, the equipment A101 transmits the response rA to equipment B102. Similarly, the equipment B102 transmits a response rB to the equipment A101. Next, the equipment A101 calculates h(kAverbar verbar nB) by using random numbers kA, nA and nB and verifies that the result is equal to the response rB received from the equipment B102. Then, the equipment A101 verifies a certifier certB of the equipment B102 by using a public key PLA of a key management organization 131. When the verification result is correct, the equipment A101 cortifies that the equipment B102 is the right equipment.